0318045-SNY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-242224

(43)Date of publication of application : 17.09.1996

(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G09C 1/00

(21)Application number : 07-044515

(22)Date of filing : 03.03.1995

(71)Applicant : MEYA TATSUHIRO

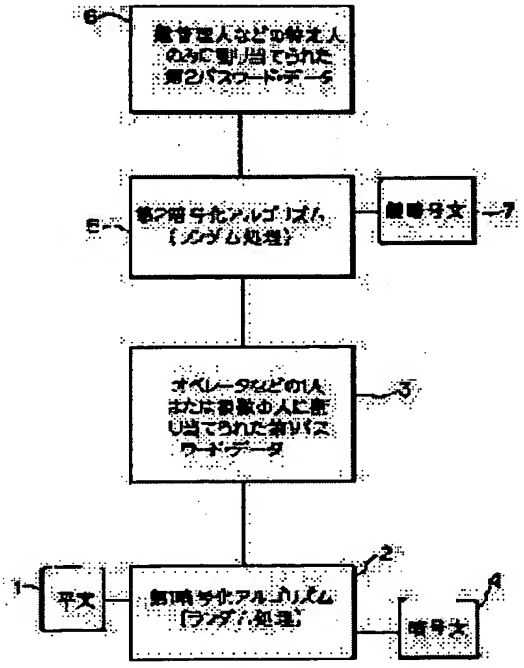
(72)Inventor : MEYA TATSUHIRO

(54) METHOD FOR CONSTRUCTING SECURITY

(57)Abstract:

PURPOSE: To construct highly advanced security.

CONSTITUTION: First prescribed ciphering algorithm 2 is applied to the data of a normal sentence 1 and a ciphered sentence 4 is generated from the normal sentence 1 by executing randomizing processing based upon 1st pass word data 3 allocated to one or plural persons. On the other hand, randomizing processing is executed once or more by the use of 2nd prescribed ciphering algorithm 5 which is the same or different as/from the 1st ciphering algorithm 2 based upon 2nd pass word data 6 allocated only to a specific custodian or the like as data inherent in the specific person to generate a key ciphered sentence 7 from the data 3 and the ciphered sentence 7 is stored and managed by the specific custodian or the like.



LEGAL STATUS

[Date of request for examination]	03.03.1995
[Date of sending the examiner's decision of rejection]	31.03.1999
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	11-07253
[Date of requesting appeal against examiner's decision of rejection]	28.04.1999

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－242224

(43)公開日　平成８年(1996)９月17日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/00			Ｈ０４Ｌ	9/00	Ｚ	
	9/10		7259－5Ｊ	Ｇ０９Ｃ	1/00		
	9/12						
Ｇ０９Ｃ	1/00						

審査請求　有　　請求項の数５　ＯＬ　（全５頁）

(21)出願番号　特願平7－44515

(22)出願日　平成７年(1995)３月３日

(71)出願人　595032185
女屋　遼腐
東京都町田市原町田３－７－10　ハイコート矢口301

(72)発明者　女屋　遼腐
東京都町田市原町田３－７－10　ハイコート矢口301

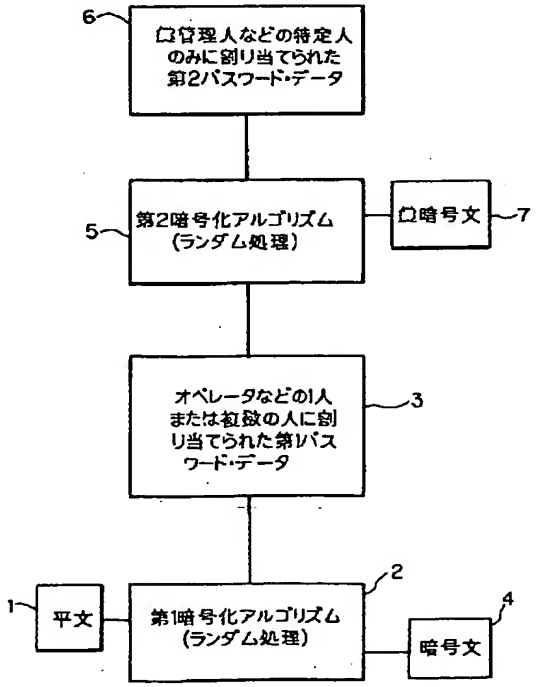
(74)代理人　弁理士　萩野　平　（外５名）

(54)【発明の名称】　セキュリティ構築方法

(57)【要約】

【目的】　より高度なセキュリティを構築することができるセキュリティ構築方法を提供することを目的とする。

【構成】　平文１のデータに対して所定の第１暗号化アルゴリズム２を使用して１人または複数の人に割り当てられた第１パスワード・データ３によりランダム化処理を行って平文１から暗号文４を生成する。また、特定の管理人などにのみに割り当てられた特定人固有の第２パスワード・データ６により、第１暗号化アルゴリズム２と同じかまたは異なる所定の第２暗号化アルゴリズム５を使用して１回以上のランダム化処理を行って、第１パスワード・データ３から鍵暗号文７を生成し、鍵暗号文７を特定の管理人などにより保管管理を行う。



【特許請求の範囲】
【請求項１】　所定の暗号化アルゴリズムを使用し、第１のパスワードデータを鍵として平文データをランダム処理し、前記平文から暗号文を生成する工程と、
特定人に割り当てられた固有の第２のパスワードデータを鍵として、前記暗号化アルゴリズムあるいはそれとは異なる所定の暗号化アルゴリズムを使用して前記第１のパスワードデータをランダム処理し、前記第１のパスワードデータから鍵暗号文を生成する工程と、からなるセキュリティ構築方法。
【請求項２】　前段工程で使用したパスワードデータを、前記各暗号化アルゴリズムの何れかあるいはそれらとは異なる所定の暗号化アルゴリズムを使用してランダム処理し、前段工程で使用したパスワードデータから鍵暗号文を生成する工程を繰り返し実行する請求項２に記載のセキュリティ構築方法。
【請求項３】　前記第２のパスワードデータが、少なくとも１つの固有情報を有することを特徴とする請求項１若しくは２に記載のセキュリティ構築方法。
【請求項４】　前記第２のパスワードデータが、装置自体に割り当てられた固有情報を有することを特徴とする請求項３に記載のセキュリティ構築方法。
【請求項５】　前記第２のパスワードデータが、特定人に割り当てれた固有情報であることを特徴とする請求項３に記載のセキュリティ構築方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、例えば、パーソナルコンピュータ（以下、パソコンと略称する）などのソフトウェアの不法複製、データ通信などに供するデータの秘匿性の保護、秘密データの改ざん防止などに有効なセキュリティ構築方法に関する。
【０００２】
【従来の技術】近似、パソコンの急速な普及に伴い、パソコン通信も盛んになり、コンピュータウイルスのパソコンへの侵入のみならず、秘密伝送データのコンピュータハッカによる破壊、秘密データの改ざん、さらには、パソコン通信に限らずソフトウェアの不法複製による知的所有権の侵害などが行われる可能性が高まってきている。このようなデータの破壊やデータの不法複製、データの改ざんなどを防止すべく、従来より種々のセキュリティ対策が講じられている。この一例として、データの改ざんが行われないように、また、通信データの機密漏洩が防止されるように、平文（誰が読んでも理解できる文書）のデータの暗号化を行って、暗号文（何らかの手段を施して翻訳しなければ、読めない文章）を生成する方法が採られている。
【０００３】このデータの暗号化に際して、データのブロック暗号が主流をなしており、ブロック暗号化のあるアルゴリズムを公開しているものとして、例えば、ＤＥＳ（Data Encryption Standard：データ暗号化規格）とＦＥＡＬ（Fast Data Encipherment Algolithm：高速データ暗号化アルゴリズム）と呼ばれる暗号化アルゴリズムがある。
【０００４】ＤＥＳ及びＦＥＡＬは、暗号化アルゴリズムを公開したアルゴリズム公開型暗号化法であり、暗号化に際して秘密鍵と称されるパスワードデータを用いている。
【０００５】
【発明が解決しようとする課題】上述のように、データの暗号化に際して、従来から種々の暗号化アルゴリズムが利用されている。ＤＥＳ及びＦＥＡＬは、秘密鍵を用いた公開型暗号化法であるが秘密鍵の管理が万全でなければ、秘密鍵が不特定人に知られてしまい、容易に暗号文が解読されてしまう。データのセキュリティを構築する場合、不特定多数のオペレータがパソコンを使用し、秘匿性を保持すべきデータをパソコンのディスクファイルに保管しておくような場合には、データが上述のように暗号化されいても、不特定多数のオペレータの中に鍵を入手できる者がいれば、暗号文を解読することができる。このように、データのセキュリティを構築する場合、暗号化アルゴリズムを強化することは勿論のこと、データの暗号化のための秘密鍵の管理を重視して初めて、システム全体の安全なセキュリティが構築される。
【０００６】本発明は、上記事情に鑑みなされたものであり、より高度なセキュリティを構築することができるセキュリティ構築方法を提供することを目的とする。
【０００７】
【課題を解決するための手段】上記目的を達成するために、本発明は、所定の暗号化アルゴリズムを使用し、第１のパスワードデータを鍵として平文データをランダム処理し、前記平文から暗号文を生成する工程と、特定人に割り当てられた固有の第２のパスワードデータを鍵として、前記暗号化アルゴリズムあるいはそれとは異なる所定の暗号化アルゴリズムを使用して前記第１のパスワードデータをランダム処理し、前記第１のパスワードデータから鍵暗号文を生成する工程とからなる。さらに、前段工程で使用したパスワードデータを、前記各暗号化アルゴリズムの何れかあるいはそれらとは異なる所定の暗号化アルゴリズムを使用してランダム処理し、前段工程で使用したパスワードデータから鍵暗号文を生成する工程を繰り返し実行するものである。さらに、前記第２のパスワードデータが、少なくとも１つの固有情報から成るものである。さらに、前記第２のパスワードデータが、装置自体に割り当てられた固有情報を有するものである。若しくは、前記第２のパスワードデータが、特定人に割り当てれた固有情報である。
【０００８】
【作用】上記構成によれば、平文のデータを所定の暗号化アルゴリズムを使用して所定の人に割り当てられた第

１パスワードデータによりランダム化処理を行い、平文のデータから暗号文を生成する。さらに、暗号文生成時に使用したのと同じ暗号化アルゴリズムあるいはそれとは異なる暗号化アルゴリズムを使用して第１パスワードデータを特定人のみに割り当てられた特定人固有の第２パスワードデータによりランダム化処理を実行して、第１パスワードデータから鍵暗号文を生成し、平文の暗号文に対する鍵を第１、第２パスワードデータによるランダム化処理で２重の暗号化を行うことにより、暗号文の解読をより一層難解なものにするとともに、システム全体が固有の情報でのみ有効な働きをするシステムセキュリティが成立する。鍵のランダム化処理は、必要に応じて多数回実行することができる。例えば、前工程で使用したパスワードデータを第３パスワードデータによりランダム化処理を実行して新たな鍵暗号文を生成することにより、平文の暗号文に対する鍵を第１、第２さらに第３パスワードデータによるランダム化処理で多重の暗号化を実行することができる。

【０００９】

【実施例】以下、本発明のセキュリティ構築方法の実施例について図面に基づき説明する。図１はその一実施例を説明するための暗号文作成のための処理手順を示す説明図である。図１における１は、平文であり、この平文１は、例えばパソコン通信などに供するものである。この平文１のデータを伝送するに際し、あるいは任意に使用するのに、データの秘匿性を保持するために、まず、平文１のデータの暗号化を行う。このデータの暗号化を行うには、従来より公知のＤＥＳまたはＦＥＡＬに使用される暗号化アルゴリズム、あるいはその他の任意のデータの暗号化アルゴリズム２（以下、第１暗号化アルゴリズムという）を使用して、例えば、１人あるいは特定された複数のパソコンオペレータなどに割り当てられ、これらの１人あるいは特定された複数のパソコンオペレータなどのみが知り得るパスワードデータ３（以下、第１パスワードデータという）によりランダム化処理を行って暗号文４を生成する。この暗号文４は、パソコン通信を行う場合には、通信回線を通して伝送したり、あるいは所定のデータの解析用などに使用したりされる。

【００１０】このようにして得れた暗号文４は、例えば、前記の１人または複数のパソコンオペレータなど以外は解読できないように、暗号文４のために、鍵管理を行う。この鍵管理に際して、本実施例では、前記第１のパスワードデータ３に対して前記第１暗号化アルゴリズム２またはこの第１暗号化アルゴリズム２とは異なる任意の暗号化アルゴリズム５（以下、これらを含めて第２暗号化アルゴリスムという）を使用して鍵管理人や、企業の経営者などの特定の人のみに割り当てられた特定人固有のパスワードデータ（以下、第２パスワードデータという）６によりランダム化処理を行うことにより、鍵暗号文７を生成する。

【００１１】このランダム暗号化処理は、１回でもよいが、複数回行うことにより、鍵がより高い階層に存在するため、鍵の解読をより難解なものにすることができる。すなわち、暗号文４に対する第３者の復合が難解なものとなる。

【００１２】上記のように生成された鍵暗号文７は、鍵管理人や、企業の経営者などの特定人が例えば、フロッピィディスク（図示せず）などに格納して通常は金庫内に保管しておく。

【００１３】次に暗号文４の復合について述べる。鍵暗号文７の復合の説明図である。まず、鍵暗号文７の暗号の解読を行う。この場合には、第２暗号化アルゴリズム５にしたがって前記第２パスワードデータ６により鍵暗号文７の暗号の解読処理８を行うことにより、第１パスワードデータ３を読み出す。

【００１４】次いで、この第１パスワードデータ３を鍵として、暗号文４の解読を第１暗号化アルゴリズム２にしたがって行うことにより、平文１を読み出す。このようにして、平文１の復合を行う。つまり、第２パスワードデータ６、第１パスワードデータ３の２重の解読を行って暗号文４の解読を行う。したがって、暗号文を解読するために、第１のパスワードデータを得ようとしても、第１のパスワードデータ３は暗号化され鍵暗号文７として存在する。さらに、鍵暗号文７を解読するために必要な第２のパスワードデータは、特定人固有のデータである。従って、平文１に対するセキュリティは非常に高いものとなる。

【００１５】次に、本発明の適用例について図２により説明する。図２は機械Ａと機械Ｂに本発明を適用し、また、機械Ａに適用されたシステムを機械Ｃの複写した場合を示している。図２において、機械Ａ内の符号「２Ａ、４Ａ、５Ａ、７Ａ」で示す部分及び機械Ｂ内の符号「２Ｂ、４Ｂ、５Ｂ、７Ｂ」で示す部分は、それぞれ図１の符号「２、４、５、７」で示す部分に対応するものである。機械Ａに対し、本発明に係わる第１のパスワードデータ２Ａ、第２のパスワードデータ５Ａ、暗号文４Ａ及び鍵暗号文７Ａから成るシステムを導入し、また、機械Ｂに対して、同様に、本発明に係わるシステムを導入する。これにより、各機械において、それぞれ本発明に係わるセキュリティを構築することにより、各機械にはそれぞれ独自のセキュリティが構築されたことになる。いま、機械Ａにおいて、暗号文４Ａ、鍵暗号文７Ａ第１暗号化アルゴリズム２Ａ及び第２暗号化アルゴリズム５Ａが本発明が導入されていない機械Ｃに複写された場合を想定する。機械Ｃでは、暗号文を復合すべく第２の暗号化アルゴリズムを解読しようとするが、第２の暗号化アルゴリズムのパスワードデータが得られないため、暗号文４Ａの解読は不可能となる。一方、本発明に係わるシステムが導入された機械Ａ及び機械Ｂにおいて、機械Ａの暗号文Ａが機械Ｂに複写された場合を想定

する。機械Ｂのシステムは機械Ａと同一システムであるため、暗号文４Ａを解読する手順は同一である。しかし、機械Ｂにおいても、第２のアルゴリズムのパスワードデータが得られないため暗号文４Ａの解読は不可能となる。なお、本発明に係わるシステムが挿入された機械に対し、通信等の正規経路を介して暗号文を送信し、暗号文４Ａの解読を許可する場合は、送信先の機械に対して第２のアルゴリズムのパスワードデータを供与することにより、暗号文４Ａが解読される。

【００１６】図２の適用例からも明らかなように、ある所定の機械から暗号文、第１パスワードデータ、暗号化アルゴリズム、鍵暗号文を複写して、別の機械に移行して暗号文を稼働させようとしても、第２パスワードデータが得られない限り、第１パスワードデータをとり出すことができないので、暗号文の解読が不可能である。したがって、暗号文のデータの保護が可能となる。また、正規のユーザによる機械Ａから機械Ｂへの通信データなどに対しては、機械Ｂが機械Ａで使用した第２のパスワードデータを享受することにより、暗号文の解読が可能である。

【００１７】なお、前記実施例および前記適用例の説明において、第２のパスワードデータとしては、パソコン自体に割り当てられた固有情報であるシリアルナンバ若しくは特定人に割り当てられた固有情報であるＩＤ番号またはそれらを組み合わせた複合データによるパスワードデータでもよい。

【００１８】

【発明の効果】以上のように、本発明によれば、所定の暗号化アルゴリズムを使用して、１人または複数の所定の人に割り当てられた第１パスワードデータにより平文のデータのランダム化処理を行って暗号文を生成し、特定人のみに割り当てられた特定人固有の第２パスワードデータにより第１パスワードデータを所定のアルゴリズムを使用して、少なくとも１回のランダム化処理を行って第１パスワードデータから鍵暗号文を生成するようにしたので、小さなキーワードデータにより、容量の大きいデータの暗号化と高度な個人認識とが可能化となる。また、データの改ざん、不法複製の防止、秘匿性の確保、などを確実に行うことができる。これにともない、製品やプログラムの使用許諾への道を開くことができるとともに、コピープロテクション、管理データの保全など様々なところで応用することがができる。

【図面の簡単な説明】

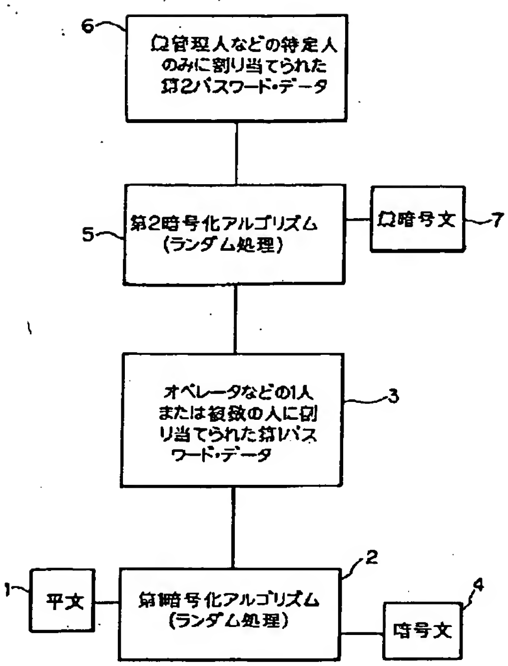
【図１】本発明のセキュリティ構築方法の一実施例の暗号化処理手順を示す説明図である。

【図２】本発明のセキュリティ構築方法の適用例の説明図である。

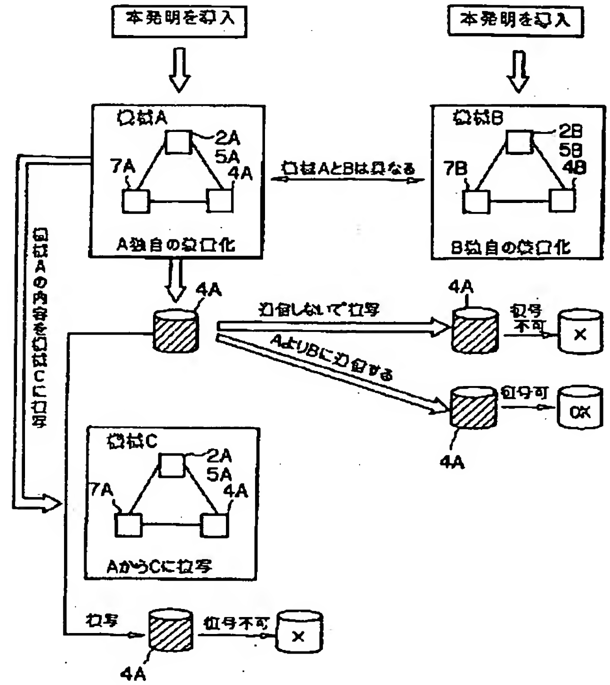
【符号の説明】

１　　平文
２　　第１暗号化アルゴリズム
３、３Ａ、３Ｂ　　第１パスワードデータ
４、４Ａ、４Ｂ　　暗号文
５　　第２暗号化アルゴリズム
６、６Ａ、６Ｂ　　第２パスワードデータ
７、７Ａ、７Ｂ　　鍵暗号文

【図１】


6
のみに割り当てられた
第2暗号化アルゴリズム
(ランダム処理)
5
7
オペレータなどの1人
ワード・データ
3
2
1
平文
(ランダム処理)
4
暗号文

【図２】


2A
5A
4A
7A
2B
5B
4B
7B
4A
×
OK
×
4A
4A
4A